

(11)Publication number : 2002-208965

(43)Date of publication of application : 26.07.2002

(51)Int.Cl.

H04L 12/66
G06F 13/00
G06F 15/00
H04L 9/32

(21)Application number : 2001-000062

(71)Applicant : NEC CORP
NTT COMMUNICATIONS KK

(22)Date of filing : 04.01.2001

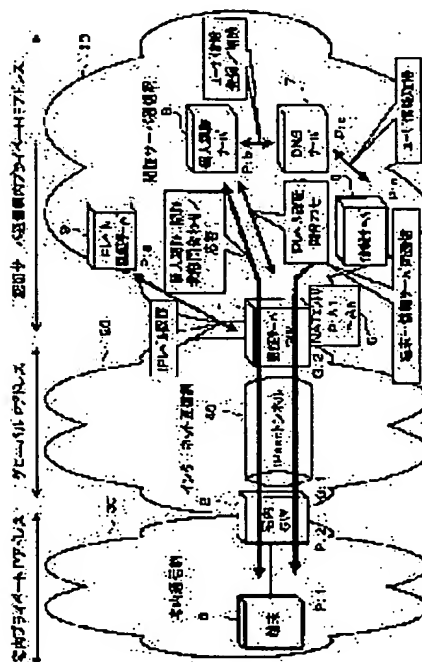
(72)Inventor : KANO OSAMU
INOUE TAKUYA
MIZOGUCHI YOICHI

(54) INTERNET RELAY CONNECTION SYSTEM.

(57)Abstract:

PROBLEM TO BE SOLVED: To achieve high level security at the time of authenticating a terminal connected from a home communication network to the Internet by dial-up, and an IP address is assigned according to the connection.

SOLUTION: An IP sec tunnel is set in a communication path in the Internet communication network so that the secured communication can be performed through the IPsec tunnel between a home communication network and an authentication server communication network. Moreover, authentication strength can be enhanced by the two stages of the IP level authentication of the IPsec tunnel establishment and the personal identification of an information server access, and a consumer can be specified from the IP address according to the linkage of an authentication server GW, an IP level authentication server, and a personal identification server. The consumer information can be acquired from the access IP address by an information server.



LEGAL STATUS

[Date of request for examination]

01.02.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-208965

(P 2002-208965 A)

(43) 公開日 平成14年7月26日 (2002.7.26)

(51) Int. Cl.	識別記号	F I	テ-マコード (参考)
H04L 12/66		H04L 12/66	B 5B085
G06F 13/00	351	G06F 13/00	351 Z 5B089
15/00	330	15/00	330 B 5J104
H04L 9/32		H04L 9/00	673 A 5K030

審査請求 有 請求項の数12 O L (全9頁)

(21) 出願番号 特願2001-62 (P 2001-62)

(22) 出願日 平成13年1月4日 (2001.1.4)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(71) 出願人 399035766

エヌ・ティ・ティ・コミュニケーションズ
株式会社

東京都千代田区内幸町一丁目1番6号

(72) 発明者 加納 修

東京都港区芝五丁目7番1号 日本電気株
式会社内

(74) 代理人 100078237

弁理士 井出 直孝 (外1名)

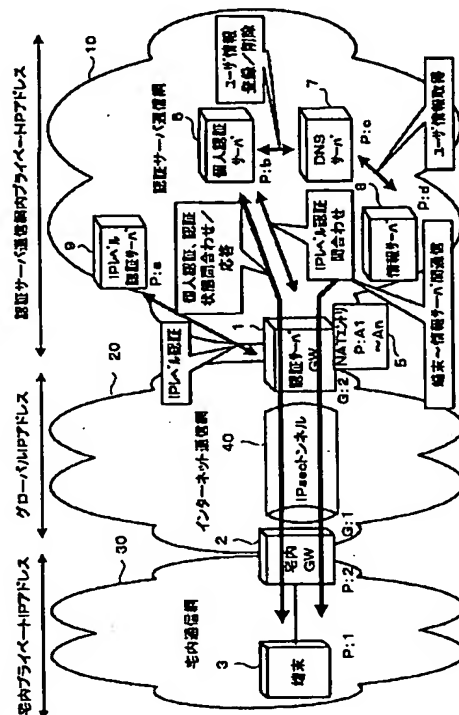
最終頁に続く

(54) 【発明の名称】 インターネット中継接続方式

(57) 【要約】

【課題】 宅内通信網からダイアルアップによりインターネットに接続され、接続によりIPアドレスがアサインされる端末の認証について、そのセキュリティを高度化する。

【解決手段】 インターネット通信網内の通信路にIPsecトンネルを設定し、宅内通信網と認証サーバ通信網との間にIPsecトンネルによるセキュアな通信を可能とする。さらに、IPsecトンネル確立のIPレベル認証と情報サーバアクセスの個人認証の二段階により、認証強度を高め、認証サーバGW、IPレベル認証サーバ、個人認証サーバの連携により、IPアドレスからコンシューマを特定し、情報サーバはアクセスしてきたIPアドレスからコンシューマ情報を取得する。



【特許請求の範囲】

【請求項1】 ダイアルアップによりインターネット・

- ・ プロトコル (IP, internet protocol) に準拠するアドレスが付与され、端末を含む宅内通信網とグローバル
 - ・ アドレスによりインターネット・プロトコルに基づく通信を行うインターネット通信網との接続点に設けられた宅内GW (Gate Way) と、
- 複数の認証サーバを含みインターネット・プロトコルに準拠するプライベートIPアドレスにより制御される認証サーバ通信網 (CSN, Certified Server Network) と前記インターネット通信網との接続点に設けられた認証サーバGW (Gate Way) とを備えたインターネット中継接続方式において、

前記インターネット通信網の中に前記宅内GWと前記認証サーバGWとの間に、IPsec (internet protocol security) トンネルを設定する手段を備えたことを特徴とするインターネット中継接続方式。

【請求項2】 前記IPsecトンネルはOSI (open system interconnection)第3層に設定された暗号化通信方式により構築された請求項1記載のインターネット中継接続方式。

【請求項3】 前記認証サーバGWは、多数のプライベートIPアドレスをプールしておくNAT (network address translator) 手段と、前記トンネルが設定されたときにそのNAT手段にプールしてあるプライベートIPアドレスを通信に関わる前記宅内通信網に属する端末に割り振る手段と、前記端末から到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって対応する認証サーバ通信網内のサーバにルーティングする手段と、前記認証サーバ通信網内のサーバから到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって前記IPsecトンネルを介して対応する端末にルーティングする手段とを含む請求項2記載のインターネット中継接続方式。

【請求項4】 前記認証サーバ通信網の中に、個人認証を行う個人認証サーバおよびドメイン名の管理を行うDNS (domain name system) サーバを少なくとも一つずつ含み、前記個人認証サーバは個人認証を実行した端末のユーザ情報を前記DNSサーバに引き渡す手段を備え、前記DNSサーバはそのユーザ情報を登録する手段を備えた請求項3記載のインターネット中継接続方式。

【請求項5】 前記登録する手段には、ユーザ識別子 (ID)、認証の有効期限、およびサービス・カテゴリの情報を登録する手段を含む請求項4記載のインターネット中継接続方式。

【請求項6】 前記認証サーバ通信網にある一つの情報サーバが前記端末の一つからアクセスを受けたときに、前記DNSサーバに対してその端末に割り振られた前記プライベートIPアドレスをキーとして問い合わせを行う手段と、この問い合わせに対して前記個人認証サ

ーバに登録されたその端末に関する情報をその問い合わせを行った情報サーバに渡す手段とを備えた請求項5記載のインターネット中継接続方式。

【請求項7】 前記個人認証サーバは、前記DNSサーバに対し、個人認証状態を終了した端末に関する情報を削除する要求を行う手段を含み、

前記DNSサーバは、当該要求にしたがって該当する情報を削除する手段を含む請求項6記載のインターネット中継接続方式。

【請求項8】 前記端末には、前記個人認証サーバからの認証の通知に対応して認証中を意味する表示をその端末の表示装置に表示する手段を含む請求項4記載のインターネット中継接続方式。

【請求項9】 前記端末には前記個人認証サーバに対して認証状態の問い合わせを行う手段を備え、前記個人認証サーバにはこの問い合わせに対して認証状態を応答する手段を備えた請求項8記載のインターネット中継接続方式。

【請求項10】 前記個人認証サーバには、認証中にある端末について前記認証状態の問い合わせがあったときにはその問い合わせから所定時間だけその認証状態を維持する手段を含む請求項9記載のインターネット中継接続方式。

【請求項11】 前記個人認証サーバには、認証中にある端末から認証終了の要求を受けたときにその認証状態を終了させる手段を備えた請求項9記載のインターネット中継接続方式。

【請求項12】 前記認証サーバGWには、一つの端末からHTTP (hypertext transfer protocol)によるアクセスがあったときにその端末の個人認証が未認証であるときにはその端末を認証を促すための認証ページに誘導する手段を備えた請求項4記載のインターネット中継接続方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、宅内通信網内のダイアルアップ環境下にある端末と、認証サーバ通信網内にあり情報提供源となる情報サーバとが、インターネットを介して接続するための中継接続に利用する。本発明は、IP (internet protocol) による通信のセキュリティ (IPsec, internet protocol security) を高度化する技術に関する。本発明は、異なるネットワーク間のアドレス変換 (NAT, network address translation) に関する。

【0002】

【従来の技術】インターネットの普及により、インターネットを利用したビジネスやサービスが加速度的に増加し、盗聴や「なりすまし」などを防止する通信のセキュリティがきわめて重要になっている。高度のセキュリティを行うために通信相手の正当性を確認するための認証

および他人に通信を盗聴されないための暗号化などがさまざまな利用されている。

【0003】このために、インターネットおよびISP (internet service provider)を経由した端末と情報サーバ間に高度のセキュリティを維持して通信を行う、SSL (secure sockets layer)が知られている。SSLは国際標準化機構 (ISO) に定められたOSI (open system interconnection)第5層にあたるプロトコルである。

【0004】

【発明が解決しようとする課題】近年、宅内通信網からダイヤルアップ接続によりインターネットを経由して、情報提供その他のサービスを受けることができるようになった。そして宅内通信網内の端末には、インターネット・プロトコルによるアドレスが固定的に付与されず、その端末がダイヤルアップにより接続されたときにインターネット・プロトコルによるアドレスがアサインされ、その接続が終了したときには、そのアドレスはまた他の端末にアサインされるようにして利用されるものが普及することになった。

【0005】そのようなアドレスについては、そのアドレスをキーとしてセキュリティを設定すると、かりにインターネット網の中で接続の終了および再接続が行われることがあると、その宅内通信網に無関係の端末による「なりすまし」が可能になる。すなわち宅内通信網内の端末がインターネットを介して認証サーバにアクセスする場合に、従来のセキュリティに加えて宅内通信網の外部からの侵入を防ぐためのセキュリティの強化が必要である。

【0006】本発明は、このような背景に行われたものであって、宅内通信網からダイヤルアップ接続によりインターネットを経由して、認証サーバにアクセスする通信接続に対して、インターネット網内のセキュリティを強化する中継接続方式を提供することを目的とする。本発明は、このようなセキュリティを強化するとともに、認証の強度を上げることができる中継接続方式を提供することを目的とする。本発明は、さらに情報サーバがアクセスを受け付けた認証サーバ通信網内プライベートIPアドレスからユーザ情報の取得を可能とする中継接続方式を提供することにより、一度認証を行えば、認証サーバ通信網内サーバ間で、その認証情報を共有することが可能となり、ユーザはサービス提供のたびに認証情報通信の必要がない、いわゆるSSO (Single Sign On) サービスを提供することを目的とする。本発明は、端末が認証状態を把握することを可能とする中継接続方式を提供することを目的とする。本発明は、認証状態を必要な期間維持することができる中継接続方式を提供することを目的とする。本発明は、個人未認証の場合に個人認証を促すことができる中継通信方式を提供することを目的とする。本発明は、IPレベル認証の対象と個人認証の

対象を管理することができる中継接続方式を提供することを目的とする。

【0007】

【課題を解決するための手段】本発明は、ダイヤルアップによりインターネット・プロトコル (IP, internet protocol) に準拠するアドレスが付与され、端末を含む宅内通信網とグローバルアドレスによりインターネット・プロトコルに基づく通信を行うインターネット通信網との接続点に設けられた宅内GW (Gate Way) と、複数の認証サーバを含みインターネット・プロトコルに準拠するプライベートIPアドレスにより制御される認証サーバ通信網 (CSN, Certified Server Network) と前記インターネット通信網との接続点に設けられた認証サーバGW (Gate Way) とを備えたインターネット中継接続方式において、前記インターネット通信網の中に前記宅内GWと前記認証サーバGWとの間に、IPsec (internet protocol security) トンネルを設定する手段を備えたことを特徴とする。

【0008】前記IPsecトンネルはOSI (open system interconnection)第3層に設定された暗号化通信方式により構築することができる。このIPsecはOSI第3層レベルでの暗号化通信方式を利用することにより、IP上のアプリケーションであれば全てのサービスを提供することが可能になる。

【0009】また、VPN (Virtual Private Network: 仮想施設網) は主に企業の拠点間通信に用いられるが、宅内通信網と認証サーバ通信網との間にIPsecトンネルを構築することにより、認証サーバ通信網内のサーバと不特定多数の宅内通信網内の端末とのIP-VPNによるセキュアな通信を可能とする。

【0010】さらに、IPsecトンネル確立のIPレベル認証と情報サーバアクセスの個人認証のレイヤの違う認証システムを連携することによりスムーズなサービス提供を可能とする。すなわち、認証サーバGW、IPレベル認証サーバ、個人認証サーバの連携により、IPアドレスからユーザを特定し、情報サーバはアクセスしてきたIPアドレスからユーザ情報を取得することができるようになる。

【0011】すなわち、本発明は、端末と情報サーバ間の異レイヤ間認証連携によるスムーズなエンドツーエンド (end to end) 通信における端末と情報サーバとの間の通信を行うためのアドレス割当技術、IPレベル認証と個人認証が連携した認証技術、認証サーバGWのNAT機能での個人認証状態の管理技術、情報サーバがアクセスしたユーザ情報の取得技術、ならびに端末に情報サーバへアクセスが可能であるかどうかの認証状態の表示技術を提供する。また、一度の認証で複数のサービスを利用できるSSOサービスをアプリケーションプロトコルに依存せず、IPレイヤレベルで実現する。

【0012】前記認証サーバGWは、多数のプライバー

トIPアドレスをプールしておくNAT (network address translator) 手段と、IPsecトンネルが設定されたときにそのNAT手段にプールしてあるプライベートIPアドレスを通信に関わる前記宅内通信網に属する端末に割り振る手段と、前記端末から到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって対応する認証サーバ通信網内のサーバにルーティングする手段と、前記認証サーバ網内のサーバから到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって前記IPsecトンネルを介して対応する端末にルーティングする手段とを含むことが望ましい。

【0013】前記認証サーバ通信網の中に、個人認証を行う個人認証サーバおよびドメイン名の管理を行うDNS (domain name system) サーバを少なくとも一つずつ含み、前記個人認証サーバは個人認証を実行した端末のユーザ情報を前記DNSサーバに引き渡す手段を備え、前記DNSサーバはそのユーザ情報を登録する手段を備えることが望ましい。

【0014】前記登録する手段には、ユーザ識別子 (ID)、認証の有効期限、およびサービス・カテゴリの情報を登録する手段を含むことが望ましい。

【0015】前記認証サーバ通信網 (CSN) 内にある一つの情報サーバが前記端末の一つからアクセスを受けたときに、前記DNSサーバに対してその端末に割り振られた前記プライベートIPアドレスをキーとして問い合わせを行う手段と、この問い合わせに対して前記個人認証サーバに登録されたその端末に関する情報をその問い合わせを行った情報サーバに渡す手段とを備えることが望ましい。

【0016】前記個人認証サーバは、前記DNSサーバに、個人認証状態を終了した端末に関する情報を削除する要求を行う手段を含み、前記DNSサーバは、当該要求にしたがって該当する情報を削除する手段を含むことが望ましい。

【0017】前記端末には、前記個人認証サーバからの認証の通知に対応して認証中を意味する表示をその端末の表示装置に表示する手段を含むことが望ましい。

【0018】前記端末には前記個人認証サーバに対して認証状態の問い合わせを行う手段を備え、前記個人認証サーバにはこの問い合わせに対して認証状態を応答する手段を備えることが望ましい。

【0019】前記個人認証サーバには、認証中にある端末について前記認証状態の問い合わせがあったときにはその問い合わせから所定時間だけその認証状態を維持する手段を含むことが望ましい。

【0020】前記個人認証サーバには、認証中にある端末から認証終了の要求を受けたときにその認証状態を終了させる手段を備えることが望ましい。

【0021】前記認証サーバGWには、一つの端末からHTTPによるアクセスがあったときにその端末の個人

認証が未認証であるときにはその端末を認証を促すための認証ページに誘導する手段を備えることが望ましい。

【0022】

【発明の実施の形態】本発明実施例のインターネット中継接続方式の構成を図1を参照して説明する。図1は本発明実施例のインターネット中継接続方式の全体構成図である。

【0023】本発明は、図1に示すように、ダイアルアップによりインターネット・プロトコルに準拠するアドレスが付与され、端末3を含むインターネット・プロトコルに準拠するプライベートIPアドレスにより制御される宅内通信網30とグローバルアドレスによりインターネット・プロトコルに基づく通信を行うインターネット通信網20との接続点に設けられた宅内GW2と、複数の認証サーバを含みインターネット・プロトコルに準拠するプライベートIPアドレスにより制御される認証サーバ通信網10とインターネット通信網20との接続点に設けられた認証サーバGW1とを備えたインターネット中継接続方式である。

【0024】ここで、本発明の特徴とするところは、インターネット通信網20の中に宅内GW2と認証サーバGW1との間に、IPsecトンネル40を設定するところにある。本発明実施例のインターネット中継接続方式の特徴を以下に列挙する。

【0025】認証サーバGW1は、多数のプライベートIPアドレスをプールしておくNAT機能5を備え、IPsecトンネル40が設定されたときにそのNAT機能5にプールしてあるプライベートIPアドレスを通信に関わる宅内通信網30に属する端末3に割り振り、端末3から到来する通信パケットをその通信パケット内の宛て先アドレスにしたがって対応する認証サーバ通信網10内の各サーバにルーティングし、認証サーバ通信網10内の各サーバから到来する通信パケットをその通信パケット内の宛て先アドレスにしたがってIPsecトンネル40を介して対応する端末にルーティングする。

【0026】認証サーバ通信網10の中に、個人認証を行う個人認証サーバ6およびドメイン名の管理を行うDNS (domain name system) サーバ7を少なくとも一つずつ含み、個人認証サーバ6は個人認証を実行した端末のユーザ情報をDNSサーバ7に引き渡し、DNSサーバ7はそのユーザ情報を登録する。この登録には、ユーザ識別子 (ID)、認証の有効期限、およびサービス・カテゴリの情報を登録する。

【0027】IPレベル認証により正当性が認証されると、IPsecトンネル40を確立し、その後個人認証サーバ6により個人認証を行う。個人認証サーバ6はNAT機能5により割り振られたプライベートIPアドレスであるアクセス元 (発) IPアドレスをキーに認証サーバGW1にIPレベル認証のユーザを問い合わせる。個人認証サーバ6は、その問い合わせ結果と自分で保持

している個人認証情報からIPレベル認証と個人認証間の整合性のチェックを行い、問題なければ個人認証の正当性を認証する。また、DNSサーバ7に対してアクセス元(発)IPアドレスをキーとしてドメインにユーザID、有効期限等のユーザ情報を適用しDNSの登録を行い、その後、ユーザからアクセスがあった情報サーバはアクセス元(発)IPアドレスをキーにDNSサーバに問い合わせを行い、その応答としてユーザ情報を含むドメイン名を取得する。

【0028】個人認証サーバ6は、DNSサーバ7に、個人認証状態を終了した端末3に関する情報を削除する要求を行い、DNSサーバ7は、この要求にしたがって該当する情報を削除する。

【0029】端末3には、個人認証サーバ6からの認証の通知に対応して認証中を意味する表示をその端末3の表示装置に表示する。

【0030】端末3は個人認証サーバ6に対して認証状態の問い合わせを行い、個人認証サーバ6にはこの問い合わせに対して認証状態を応答する。

【0031】個人認証サーバ6には、認証中にある端末3について前記認証状態の問い合わせがあったときにはその問い合わせから所定時間だけその認証状態を維持する。

【0032】個人認証サーバ6は、認証中にある端末3から認証終了の要求を受けたときにその認証状態を終了させる。

【0033】認証サーバGW1は、一つの端末3からHTTPによるアクセスがあったときにその端末3の個人認証が未認証であるときにはその端末3に認証を促すために、その端末3を個人認証サーバ上の認証ページに誘導する。

【0034】図1に示すネットワーク構成例を参照して本発明のインターネット中継接続方式の特徴的なシーケンスを簡単に説明すると、端末3にプライベートIPアドレスを付与する。端末3はダイヤルアップ環境でインターネットまたはISP(internet service provider)を経由して認証サーバGW1へ接続を要求する。IPレベル認証サーバ9は宅内GW2を認証し、認証が認められると宅内GW2と認証サーバGW1との間でIPsecトンネル40を確立する。認証サーバGW1はインターネットまたはISPを経由して接続する端末3を認証サーバ通信網10でユニークに扱うためにNAT機能5を有する。NAT機能5で使用するNATエントリテーブルにおいて端末3の個人認証状態を管理する。宅内通信網30、認証サーバ通信網10内はプライベートIPアドレスにより通信を行い、端末3からの認証サーバ通信網10へアクセスが発生するとプライベートIPアドレスを端末3に割り当てる。IPレベル認証を行った後、個人認証サーバ6はユーザの個人認証を行う。個人認証サーバ6は、アクセスしたプライベートIPアドレ

スからIPレベル認証を行った宅内GW2の識別情報を認証サーバGW1から取得しIPレベル認証と個人認証の関係の正当性をチェックする。IPレベル認証、個人認証を行うとIPレベル認証サーバ9と個人認証サーバ6は連携しDNSサーバ7にアクセスしたユーザ情報を登録し、情報サーバ8はDNSサーバ7に問い合わせを行い、ユーザ情報を取得する。個人認証サーバ6は個人認証の状態を端末3へ通知し、端末3は個人認証サーバ6へ認証状態の問い合わせを行う。認証サーバGW1は、個人認証を行っていない場合には、個人認証サーバ6に個人認証を促す。

【0035】以下、本発明実施例をさらに詳細に説明する。図1を参照して、本実施例は宅内通信網30内の端末3、宅内GW2、認証サーバ通信網10内の認証サーバGW1、IPレベル認証サーバ9、個人認証サーバ6、DNSサーバ7、情報サーバ8を含む。

【0036】ユーザは端末3を操作して宅内GW2を介しダイヤルアップ接続によりインターネットまたはISP(internet service provider)を経由して認証サーバ通信網10に接続する。認証サーバGW1は、宅内GW2との間でIPsecトンネル40を確立する。認証サーバGW1はNAT機能5を有し、また端末3を認証サーバ通信網10内でユニークと扱うためのプライベートIPアドレスをプールする。IPレベル認証サーバ9は、認証サーバGW1からの認証要求に対し端末3とIPsecトンネル40の確立を行うための認証を行う。個人認証サーバ6は、IPレベル認証を行った後ユーザ個人を認証する。DNSサーバ7は、ユーザ情報を保持する。ユーザ情報は、IPレベル認証サーバ9と個人認証サーバ6が連携し認証を行うと登録し、認証が終了すると削除する。情報サーバ8は認証サーバ通信網10に接続したユーザの端末3に情報を提供する。情報サーバ8はアクセスのあった端末3にNAT機能5により割り振られたプライベートIPアドレスをDNSサーバ7に問い合わせ、ユーザ情報を取得する。

【0037】次に、図1ないし図5を参照して本実施例の動作について詳細に説明する。図2は宅内GW2と認証サーバGW1との間に確立されたIPsecトンネルの概念図である。図3は異なるネットワーク間を転送されるパケットのアドレス付与状況を示す図である。図4は個人認証サーバ、DNSサーバ、情報サーバ相互間の動作を示す図である。図5は本発明実施例のインターネット中継接続方式の全体的な動作を示す図である。

【0038】宅内GW2は、ユーザが操作する端末3にプライベートIPアドレスを割り振り、ダイヤルアップ接続によりISPよりグローバルIPアドレスが割り振られる。認証サーバGW1は、端末3とのIPsecトンネル通信で使用するグローバルIPアドレスと宅内の端末3を認証サーバ通信網10内でユニークに扱うためプライベートアドレスをプールする。宅内GW2はユー

ザの端末3からの認証サーバ通信網10内の情報サーバ8へのアクセスを検出すると、宅内GW2と認証サーバGW1間にグローバルIPアドレスを使用したIPsecトンネル40の確立を要求する。

【0039】認証サーバGW1は宅内GW2とIPsecトンネル40の接続可否を、IPレベル認証サーバ9に問い合わせる。IPレベル認証サーバ9は、宅内GW2の認証を行い、宅内GW2と認証サーバGW1との間のIPsecトンネル40の確立可否を応答する。確立可の場合には宅内GW2と認証サーバGW1との間でグ

ローバルIPアドレスを使用したIPsecトンネル40を確立する。

【0040】IPsecトンネル40を確立すると、ブールしてある認証サーバ通信網10内のプライベートIPアドレスを割り振る。認証サーバGW1は、NAT機能5により図のように認証サーバ通信網10内のプライベートIPアドレスを管理することでユーザの端末3を認証サーバ通信網10内でユニークとする。NAT機能5ではIPsec確立要求を受け付けた各端末毎に個人認証状態を管理する。

【0041】NAT機能5のNATエントリ情報で管理している個人認証状態が個人認証未である場合には、個人認証サーバ6の個人認証ページに誘導することで個人認証をユーザに促す。

【0042】その個人認証サーバ6は、認証サーバGW1と連携してIPレベル認証の識別情報と個人認証の識別情報の組み合わせ関係の正当性をチェックし、ユーザに割り振った認証サーバ通信網10内のプライベートIPアドレスをキー情報としてDNSサーバ7に個人の識別情報、有効期限、サービスカテゴリのユーザ情報を登録する。個人認証サーバ6は個人認証を正常に行ったことを認証サーバGW1へ通知し、認証サーバGW1はNAT機能5で使用するNATエントリ情報で個人認証状態を管理する。このようにして、ユーザの情報サーバ8へのアクセス可否を判定する。アクセス可であればユーザに情報サーバ8へのアクセスを許し、そうでなければユーザにアクセスを拒否したことを通知する。

【0043】個人認証サーバ6は、個人認証を行いアクセスが許可されたことを端末3に通知する。端末3は個人認証サーバ6からの通知にしたがい、認証状態(認証中)を端末画面に表示する。端末3は認証状態を定期的に個人認証サーバ6に問い合わせ、個人認証サーバ6がそれに応答することで端末3および個人認証サーバ6で連携して認証状態の相互確認を行う。個人認証サーバ6は端末3からの認証状態問い合わせにより、認証状態を継続し続ける。

【0044】端末3から認証サーバ通信網10内の情報サーバ8へのパケットは、宅内GW2で暗号カプセル化しIPsecトンネル40を使用して認証サーバGW1に送信する。このとき、暗号カプセル化しているパケッ

トは、発アドレスは端末3の宅内通信網30のプライベートアドレス、着アドレスは情報サーバ8の認証サーバ通信網10内のプライベートIPアドレスである。認証サーバGW1は、暗号カプセル化しているパケットを復号して取り出し、NAT機能5の管理情報にしたがい、発アドレスを端末3の宅内通信網30内のプライベートアドレスからユニークな認証サーバ通信網10内のプライベートIPアドレスに付け替えを行い、情報サーバ8へパケットを送信する。

【0045】情報サーバ8から端末3へのパケットは、認証サーバGW1のNAT機能5で逆のアドレス付け替えを行い、認証サーバGW1でパケットを暗号カプセル化して宅内GW2へ送信し、宅内GW2で復号してパケットを取り出し転送する。

【0046】情報サーバ8は、DNSサーバ7にアクセスしてきた認証サーバ通信網10内のプライベートIPアドレスをキーとしてDNSサーバ7に問い合わせることでアクセスしてきたユーザの情報を取得する。

【0047】端末3が情報サーバ8と個人認証状態を終了するとき、端末3から個人認証サーバ6に認証中状態の終了を要求する。個人認証サーバ6は、DNSサーバ7に対し認証状態を終了するユーザの情報をDNSサーバ7から削除するため、削除要求を行う。このとき、個人認証サーバ6自身の個人認証状態をクリアする。また、個人認証サーバ6は、端末3からの認証状態問い合わせを監視し、一定期間認証状態問い合わせがないことを検出し認証状態の終了を行う。さらに、端末3が認証サーバ通信網10内で使用していたプライベートIPアドレスのNAT情報はクリアされる。

【0048】認証サーバ通信網10内のプライベートIPアドレスを割り当てる手段として、端末3から最初のアクセスがあったときに認証サーバ通信網10内のプライベートIPアドレスを割り当てる。

【0049】個人認証未の場合の個人認証を促す手段として、端末3がHTTP以外のプロトコルを使用している場合には、端末3に専用APLを配備し端末3の専用APLに個人認証を要求する。

【0050】

【発明の効果】以上説明したように、本発明の第一の効果として、宅内GWと認証サーバGW間にIPsecトンネルを確立することにより、端末と情報サーバ間のセキュアな通信を可能とする。

【0051】第二の効果は、認証サーバGWにNAT機能を具備することにより、グローバルIPアドレスが変わるダイヤルアップ環境での宅内と認証サーバ通信網間のセキュアな通信を可能とする。

【0052】第三の効果として、IPレベル認証と個人認証の二段階による認証により、認証の強度を上げることを可能とする。

【0053】第四の効果として、認証状態の開始または

11

終了に合わせてDNSサーバへユーザ情報登録または削除を行うことにより、情報サーバはアクセスを受け付けた認証サーバ通信網内プライベートIPアドレスからユーザ情報の取得を可能とする。これによりユーザに対して、認証サーバ通信網10内の複数のサービスを利用する際、その都度認証を行う必要がない、いわゆるSSOサービスの提供を可能とする。

【0054】第五の効果として、端末と個人認証サーバの連携により、端末が認証状態を把握することを可能とする。

【0055】第六の効果として、端末と個人認証サーバの連携により、認証状態を維持することを可能とする。

【0056】第七の効果として、認証サーバGWのNATエントリ情報で個人認証状態を管理することにより、個人認証未の場合に個人認証を促すことを可能とする。

【0057】第八の効果として、認証サーバ通信網内プライベートアドレスをキー情報としたIPレベル認証と個人認証の連携により、IPレベル認証の対象と個人認証の対象を管理することを可能とする。

【図面の簡単な説明】

【図1】本発明実施例のインターネット中継接続方式の全体構成図。

12

【図2】宅内GWと認証サーバGWとの間に確立されたIPsecトンネルの概念図。

【図3】異なるネットワーク間を転送されるパケットのアドレス付与状況を示す図。

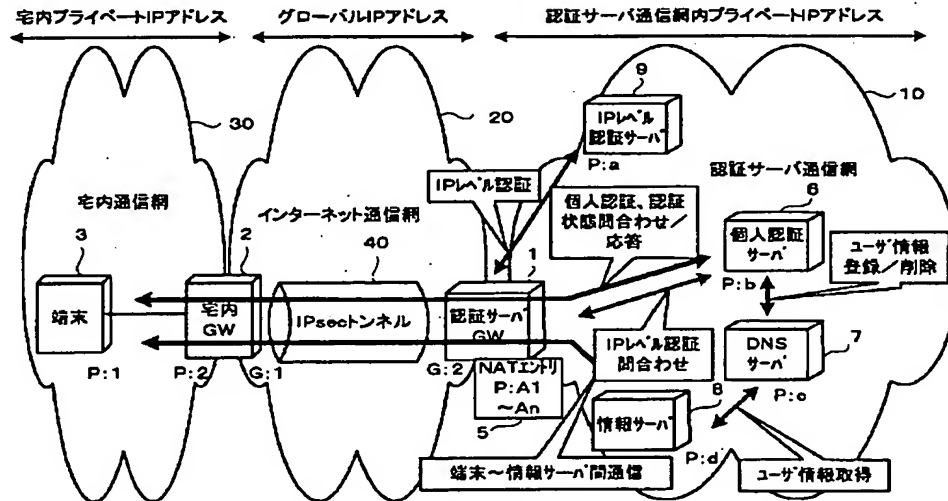
【図4】個人認証サーバ、DNSサーバ、情報サーバ相互間の動作を示す図。

【図5】本発明実施例のインターネット中継接続方式の全体的な動作を示す図。

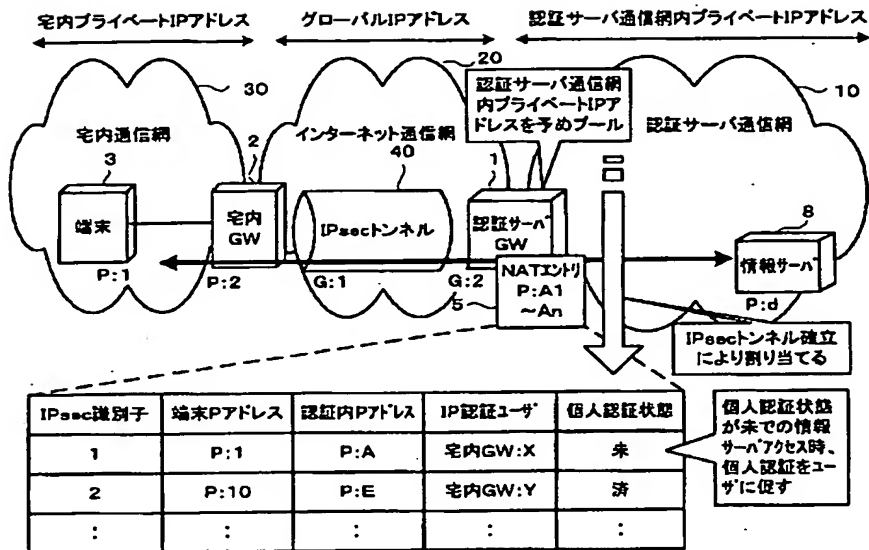
【符号の説明】

- | | |
|----|---------------|
| 10 | 1 認証サーバGW |
| | 2 宅内GW |
| | 3 端末 |
| | 5 NAT機能 |
| | 6 個人認証サーバ |
| | 7 DNSサーバ |
| | 8 情報サーバ |
| | 9 IPレベル認証サーバ |
| | 10 認証サーバ通信網 |
| | 20 インターネット通信網 |
| 20 | 30 宅内通信網 |
| | 40 IPsecトンネル |

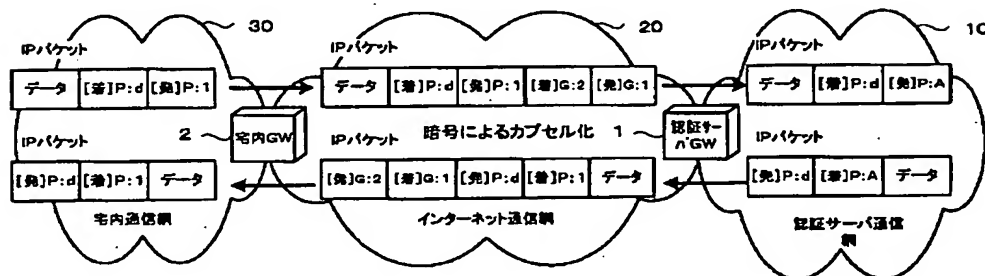
【図1】



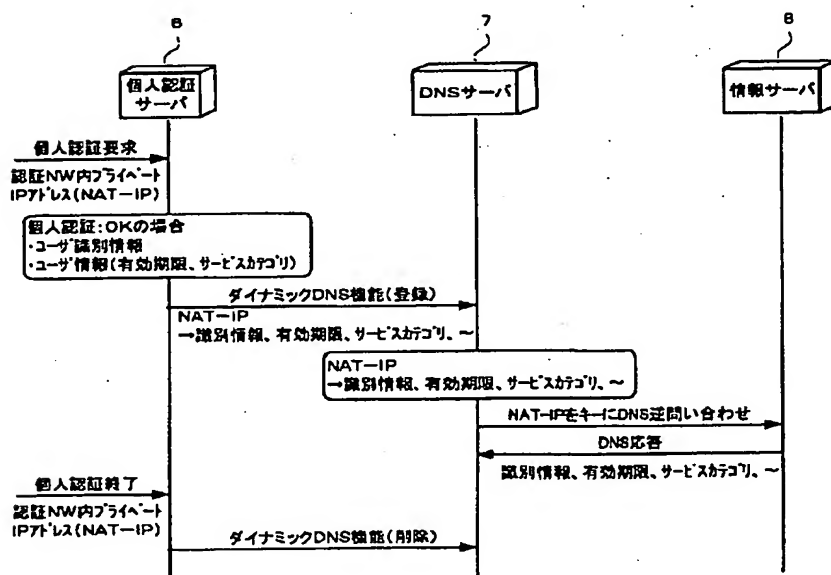
【図2】



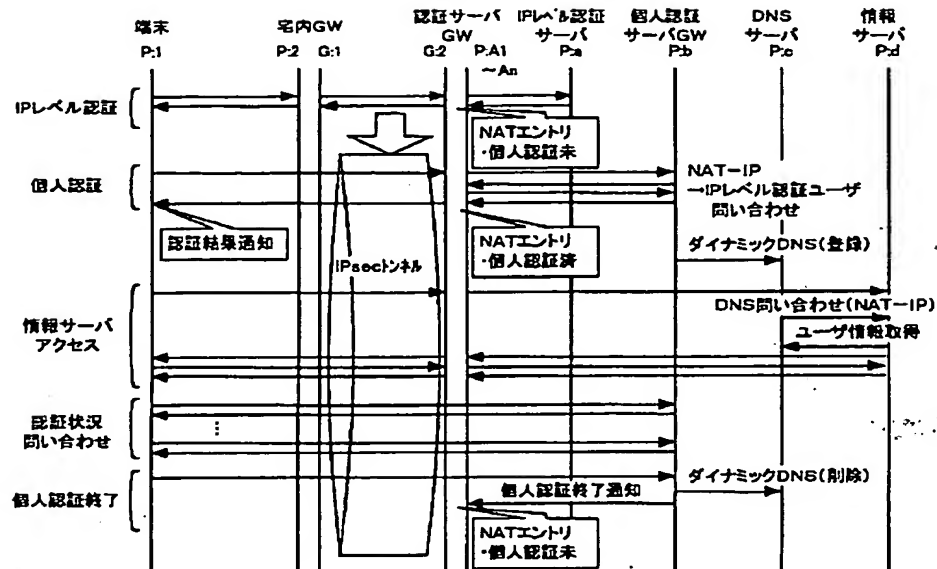
【図3】



【図4】



【図5】



フロントページの続き

(72)発明者 井上 拓也
東京都千代田区内幸町一丁目1番6号 エ
ヌ・ティ・ティ・コミュニケーションズ株
式会社内

(72)発明者 溝口 陽一
東京都千代田区内幸町一丁目1番6号 エ
ヌ・ティ・ティ・コミュニケーションズ株
式会社内

Fターム(参考) 5B085 AE02 AE23 BG07
5B089 HA10 KA17 KC58
5J104 AA07 KA01 PA07
5K030 GA15 HA08 HB18 HC01 HC13
HD03 HD06 HD09 JL07 JT06
KA04 KA13 LA07 LB15 LD19